Name: Demontae Watson

Date: 11/10/2024

Employee Training or Cybersecurity Technology: Finding a Balance

Introduction

Human error is the leading cause of cyber threats. According to Ncubukezi, “The challenge stems from the diverse range of human errors which ultimately grant unauthorized access to sensitive information and other business assets, resulting in significant data and security breaches” (2022). These human errors include things such as phishing attacks, weak passwords, social engineering, and many more behaviors and mistakes which are key contributors to cybersecurity vulnerabilities. As a Chief Information Security Officer (CISO) with a limited budget, finding a balance between where to put my funds between employee training and cybersecurity technology is important.

Employee Training

I’ve never looked into how much it would cost to effectively train employees with a focus on cyber threats, but from basic knowledge, it depends on the how many employees I have and how advanced I want the training to be. For example, I think all is needed for effective training is to send maybe bi-weekly emails out which focuses on basic cyber hygiene including having strong passwords, detection of phishing attacks, and other simple cyber threats they may face. Of course, it’s more to it, but that’s a basis of where I would start and that’s not cost effective at all. Now if I were to require each of my employees to complete some type of interactive training, that would cost a lot more than I would want especially, like I said, depending on the size of my organization.

Cybersecurity Technologies

As far as cybersecurity technology, I think this is where most of my money would go towards. Good cybersecurity technology can reduce these human errors I mentioned. For example, most websites require you to use a password of at least 8 characters comprised of numbers, letters, and special characters. This is one basic technology that can be implemented as well as not allowing for unverified emails to contact my organization's employees. Of course, I would invest in actual automated tools like Security Information and Event Management (SIEM) to better maintain security.

Summary

Overall, I understand employee training is important, but I think as far as having limited funds and having to figure it out between the two, I think having actual cybersecurity technology is much more important than doing intensive employee training that would do just as good as a meeting or regular emails on the importance of cybersecurity.

Works Cited

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395).